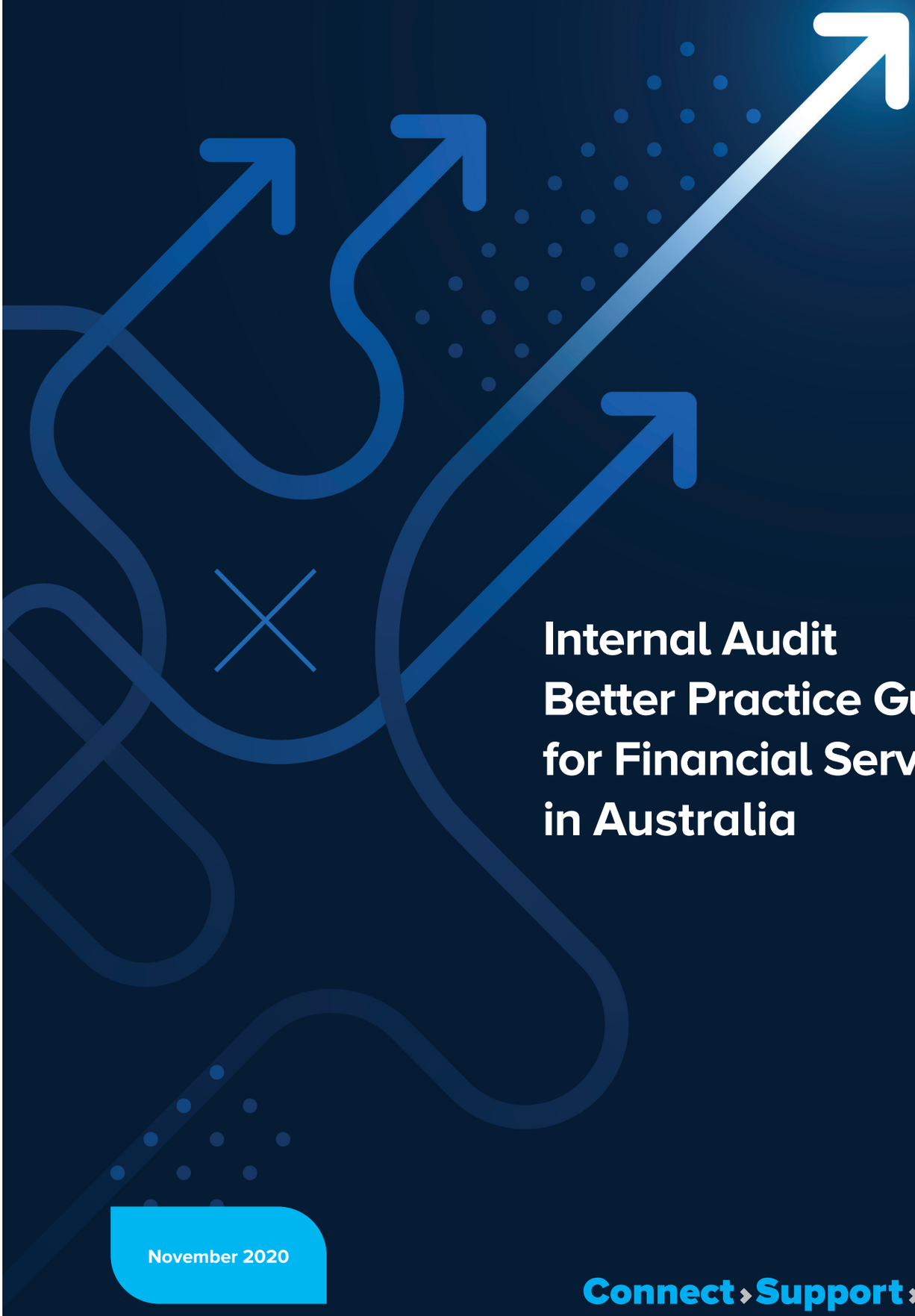
The Institute of Internal Auditors Australia



Internal Audit Better Practice Guide for Financial Services in Australia

November 2020

Connect › Support › Advance

CONTENTS

FOREWORD

The Committee to develop best practice internal audit guidance for the financial services sector has done excellent work in formulating a principles-based document. The Institute of Internal Auditors – Australia has accepted all its recommendations.

I am confident that Audit Committees and internal audit practitioners will adopt the principles contained in the Better Practice Guide, and apply them rigorously and without hesitation to achieve better governance outcomes for the sector.

The Committee, chaired by non-executive director Sandra Birkensleigh, comprised internal auditors and Audit Committee members from banking, superannuation, insurance and academia.

I would like to thank the Committee on behalf of the Institute and its members for the outstanding work they have produced.

This internal audit guide outlines activities that should be conducted in a manner consistent with the International Professional Practices Framework (IPPF, including Core Principles for the Professional Practice of Internal Auditing, the Definition of Internal Auditing, the Code of Ethics and the International Standards for the Professional Practice of Internal Auditing ('the Standards')).

The guide will also complement the ASX Corporate Governance Council's Principles and Recommendations (4th edition).

Finally, I would like to extend the gratitude of the IIA-Australia for the secretariat support provided by EY and KPMG, who were instrumental in ensuring the guidance was completed quickly and without fuss.

Peter Jones
CEO, Institute of Internal Auditors – Australia

Message from the Chair

The Australian financial services sector has come under greater scrutiny and pressure following the Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry.

As with any Royal Commission or Prudential Inquiry into our banking and financial services, we must learn from the mistakes and quickly reform policies and procedures that achieve more effective outcomes for our customers, stakeholders and shareholders.

One clear policy failure, which was raised in APRA's Prudential Inquiry into the CBA, was the role internal audit could play in governance structures. In many instances audit reports were just ignored.

There are many more examples of internal auditors being ignored by senior management and Audit Committees.

When the Royal Commission had completed its hearings, the Institute of Internal Auditors – Australia, in responding to the Commission's Final Report, also reviewed the lessons from the banking scandals in the UK in 2013.

The Chartered Institute of Internal Auditors (UK), in response to the scandals, developed an internal audit guide for the financial services sector, issuing the first edition of *Effective Internal Audit in the Financial Services Sector* in 2013, and revising it in 2017.

A survey of the effectiveness of the guidance was undertaken in 2015 and found that, on balance, internal audit budgets, staff numbers, seniority levels and levels of training had all increased. There were also improved reporting lines for heads of internal audit to Audit Committee Chairs and secondary reporting lines to CEOs.

From Australia's point of view, the UK guidance provides a valuable blueprint for developing an effective internal audit guide for our financial services sector, which has its own unique aspects.

I am delighted by the level of engagement from the Australian financial services industry in developing our own internal audit guide.

The guide sets out what is expected of internal audit, so Boards, Audit Committees and regulators alike can set their expectations.

This internal audit guide should be applied in conjunction with the International Professional Practices Framework (IPPF) and International Standards for Professional Practice of Internal Auditing ('the Standards'), the only universally applicable standards for internal audit practitioners.

I am privileged to lead a distinguished group of industry professionals and an experienced risk governance academic to create our own guidance that will assist internal audit practitioners, senior management, Audit Committee Chairs and stakeholders to achieve our objective of improving governance structures.

The Institute has undertaken a widespread consultation process with the financial services sector to achieve this outcome. The desired aim is to improve corporate governance outcomes for the benefit of all parties.

In the end, I strongly encourage adoption of this guidance as it is the responsibility of Boards, internal auditors and senior management to ensure that best practice of the internal audit function is being achieved for the benefit of customers, stakeholders and shareholders of the entity.

Finally, I would also like to thank our observers, particularly ASIC and APRA, for their support, and EY and KPMG for their secretariat support.

Sandra Birkensleigh
November 2020

The purpose and application of the Better Practice Guide

These recommendations set out internal audit practices for financial services entities in Australia. The Committee recognises, however, that different entities may legitimately adopt different practices, based on a range of factors, including their size, complexity, history and corporate culture. For that reason, the recommendations contained in the Internal Audit Better Practice Guide for Financial Services Australia ('Better Practice Guide') are not mandatory, and do not seek to prescribe the internal audit practices that an entity must adopt.

While the recommendations apply to financial services entities, since they reflect a contemporary view of appropriate internal audit practices, other bodies may find them helpful in formulating their practices.

The recommendations should guide boards, Audit Committees and Chief Audit Executives (CAEs) in the establishment and operation of an internal audit activity.

References to the CAE should be taken to refer to a senior officer of the organisation who is responsible for effectively managing the internal audit activity.

The Chief Audit Executive is accountable for the internal audit activity's overall performance, including conformance with the Standards and other organisational requirements.

Where the CAE is relying on others to undertake the work (for example, a subordinate, a branch office, or a service provider) the CAE remains accountable for this performance.

The structure of the recommendations

The recommendations are structured around, and seek to promote, six central principles:

Principle 1 – Position internal audit for success

The primary purpose of internal audit should be to assist the Board and senior management to protect the assets, reputation and sustainability of the organisation.

Principle 2 – Ensure adequate resourcing and seniority

The composition, structure and remuneration arrangements of internal audit should support independent and effective assurance.

Principle 3 – Provide assurance which adds value

Internal audit should be effective and add value in meeting the assurance needs and expectations of the Board and stakeholders.

Principle 4 – Employ methods and tools appropriate to the task

Internal audit should maintain an up-to-date methodology and underlying practices, and associated tools, to enhance its effectiveness.

Principle 5 – Report to influence positive change

Internal audit should drive positive change by providing timely, accurate and insightful information to be used as a basis for making risk-focused decisions.

Principle 6 – Adopt appropriate methodologies for auditing risk culture

The responsibility for setting risk culture sits with the organisation's Board. Organisational management then has the accountability for driving that risk culture through the organisation, measuring and reporting on risk culture and determining actions to address any gaps. As an independent function, internal audit can provide independent assurance on the governance processes around risk culture and reporting, but also an independent view of the risk culture itself. Internal audit provides assurance in relation to risk culture both through 'business as usual' audits and broader risk culture audits.

There are 32 specific recommendations of general application intended to give effect to these principles. There is also explanatory commentary, with further guidance on the recommendations.

Where appropriate, reference is being made to the applicable International Standards for the Professional Practice (IPPF) of Internal Auditing, effective as of January 2017.

Appendix A contains an overview and explanation of the various internal audit operating models utilised across organisations in Australia.

Appendix B gives an overview of the Three Lines Model of the components of effective organisation risk management.

Appendix C is a glossary of the key terms used in this document.

PRINCIPLE 1

Position internal audit for success

The primary purpose of internal audit should be to assist the Board and senior management to protect the assets, reputation and sustainability of the organisation.

Recommendation 1.1

The role of internal audit should be articulated in an internal audit charter which is publicly available and sets out:

a. The primary purpose of internal audit; and

b. The mandate of internal audit.

Commentary:

The Audit Committee Chair should have the responsibility to approve and provide oversight of compliance with the internal audit charter.

The Board, subcommittees (including the Audit Committee) and senior management should have a defined role to set the 'tone from the top', to support internal audit in achieving its purpose, role and mandate, while promoting acceptance of internal audit across the organisation.

In general terms, the mandate of internal audit should encompass:

- Active collaboration with management and the Board to inform an understanding of the organisation's key risks, audit coverage and scope;
- Proactive challenge of executive management to improve the effectiveness of risk culture, governance, risk management and key internal controls;[1]
- Assessment of whether all significant risks are identified and appropriately reported by management and risk function to the Board; and
- Independent determination on whether internal controls are adequate, given the organisation's key risks.

IIA Standard (IPPF) references:

1000 – Purpose, Authority, and Responsibility

1 Refer to Recommendation 1.4

Recommendation 1.2

The Chief Audit Executive or Head of Internal Audit[2] should have a primary reporting line to the Chair of the Audit Committee. There may also be an administrative reporting line to the Chief Executive Officer (or direct report).

The Audit Committee should have documented responsibility for appointing and removing the CAE in the internal audit charter.

Commentary:

The CAE's reporting lines should be designed to support the preservation of independence within an organisation and promote the standing of internal audit alongside the leadership team.

The CAE should have ongoing and regular access to the Audit Committee Chair, with access to other Audit Committee Members as required. It would be prudent for an 'in-camera'[3]

session between the CAE and the Audit Committee to be held at each Audit Committee meeting.

When appointing the CAE, the Audit Committee should balance technical skills and capabilities against attributes such as courage, emotional intelligence and stakeholder management and engagement.[4]

IIA Standard (IPPF) references:

1100 – Independence and Objectivity

1110 – Organisational Independence

1111 – Direct Interaction with the Board

Recommendation 1.3

Subsidiary, branch and individual heads of internal audit should report to the group CAE, while maintaining recognition of local legislation and regulation.

Commentary:

Subsidiary, branch and divisional heads of internal audit should report primarily to the CAE, while recognising local legislation or regulation, as appropriate. This includes

the responsibility for setting budgets and remuneration, conducting appraisals and reviewing the internal audit plan.

The group CAE should consider the independence, objectivity and tenure of the subsidiary, branch or divisional heads of internal audit when performing appraisals.[5]

Recommendation 1.4

The scope of internal audit should be unrestricted and organisation-wide. At a minimum, internal audit should include the following areas within its scope:

a. Governance, risk structures and processes;

b. Risk and control culture of the organisation;

c. Risk of poor customer treatment; and

d. Key corporate events.

Commentary:

In general, the following information should be considered, to inform each scope area:

Governance, risk structures and processes

- The design and operating effectiveness of the internal governance structure and processes of the organisation;
- The specific processes and controls which support strategic and operational decision-making, and whether the information presented to the Board and leadership team appropriately represents the benefits, risks and assumptions associated with the requisite strategy and/or corresponding business model; and
- The risk management framework (as required by APRA's Prudential Standard CPS 220 and SPS 220[6]), including assessment of the quality of work prepared by first and second line management roles.

Risk and control culture of the organisation

- The manner by which the processes, actions, tone from the top and observed behaviours across the organisation are aligned with the organisation's core values, ethics, policies and risk appetite; and
- The observed attitude and approach to risk management and internal controls, including management's actions to address known control deficiencies and the continuing assessment of controls.

2 Hereinafter, such positions will collectively be referred to as the Chief Audit Executive (CAE)
3 'In-camera' refers to a session held in private
4 Refer to Recommendation 2.1(b)(v)
5 Refer to Recommendation 2.4
6 As per paragraph 45 of CPS 220 Risk Management and paragraph 27 of SPS 220 Risk Management

Risk of poor customer treatment

- Whether the organisation acts with integrity in its dealings with customers and broader interactions with the market; and
- The manner by which the business and risk management are designing and controlling products, services and supporting processes to align with customer interests and conduct regulation.

Key corporate events

- Significant business process changes, introduction of new products and services, outsourcing, acquisitions or divestments; and
- Internal audit should work in conjunction with the Chief Risk Officer and risk function on a real time basis to assess the appropriate level of internal audit involvement in corporate events which present a high risk to the organisation.

To discharge its responsibilities effectively, internal audit should have timely access to key management information and a right of access to the relevant records of the organisation.

Internal audit should not adopt a 'tick box' approach based solely on the design of processes and controls, but should rather consider the outcomes which will result from their application, as assessed against the organisation's core values, ethics, policies and risk appetite.

IIA Standard (IPPF) references:

2110 – Governance

2120 – Risk Management

2130 – Control

Recommendation 1.5

The audit universe and internal audit plan should be risk-based and independently set by internal audit, based on reasonable consultation with the organisation's stakeholders and subject to the review, challenge, and approval of the Audit Committee.

Commentary:

Internal audit should exercise its own judgement to determine the most effective segmentation of the audit universe, given the structure and risk profile of the organisation. At least annually, the completeness of the audit universe should be verified (i.e. does it capture all staff or financial hierarchies within the organisation).

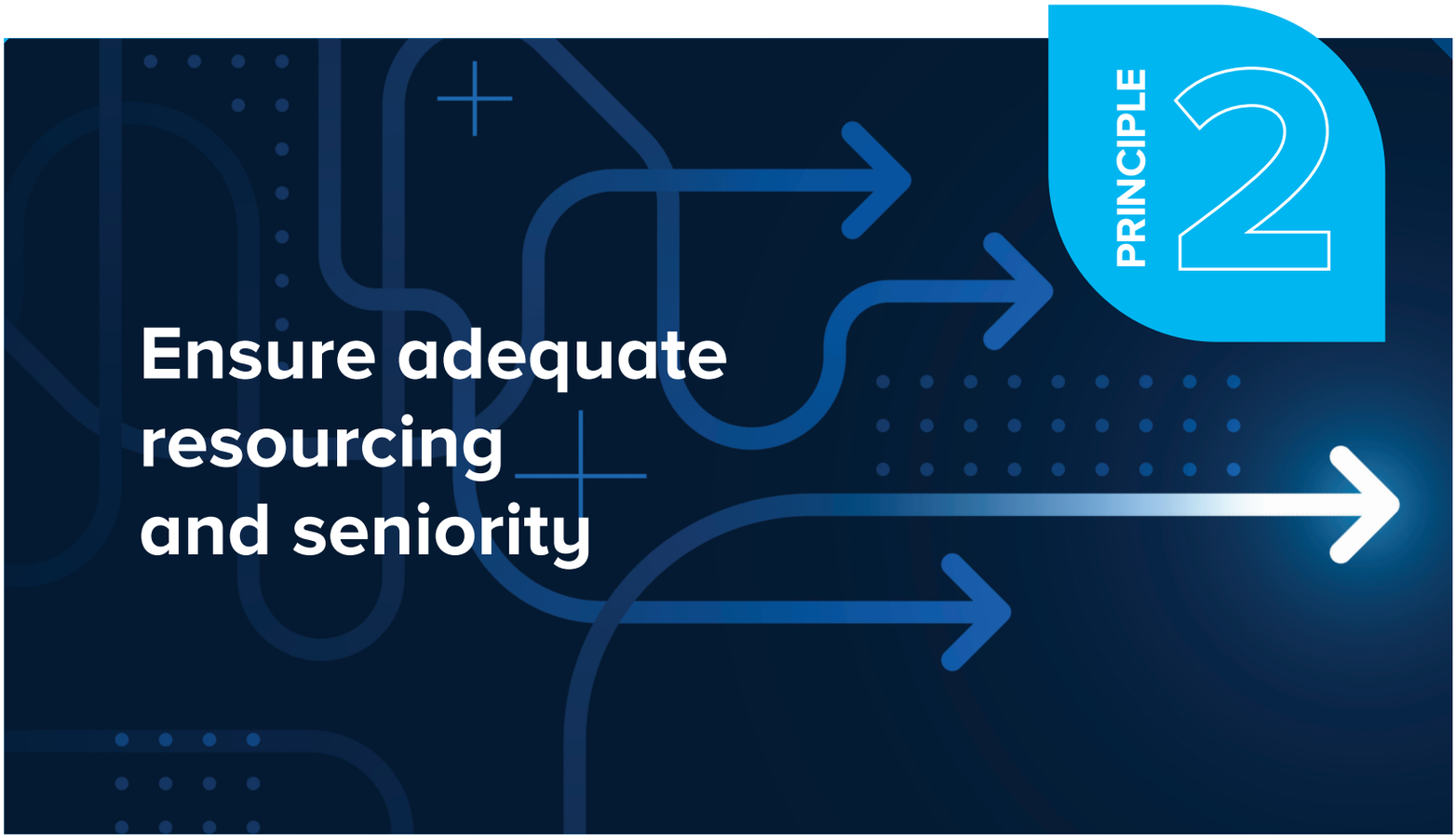
In setting out its priorities and deciding where to carry out more detailed work, internal audit should adopt a risk-based internal audit plan to focus on areas where it considers risks to be higher. The plan does not need to cover all scope areas each year, but should also not be restricted due to a lack of resources, capabilities or skills. Its judgement on which areas should be covered in the internal audit plan, and the frequency and method of audit cycle coverage, should be subject to challenge and approval by the Audit Committee.

The internal audit plan should be designed to be flexible to respond to unplanned events and allow internal audit to prioritise emerging risks, with any changes to the plan considered in light of internal audit's ongoing assessment of risk. This process should include collaboration with key stakeholders (including the Audit Committee and senior management) so as to understand the operating environment of the organisation, current and emerging risks, strategic initiatives and regulatory impacts. Any material changes made to the internal audit plan should be approved by the Audit Committee.

IIA Standard (IPPF) references:

2010 – Planning

2020 – Communication and Approval



Ensure adequate resourcing and seniority

The composition, structure and remuneration arrangements of internal audit should support independent and effective assurance.

Recommendation 2.1

The CAE must be a member of a relevant professional body with an appropriate code of professional conduct and a member disciplinary process. Examples would include the Institute of Internal Auditors (IIA) and Chartered Accountants Australia and New Zealand (CA ANZ). The CAE should ensure that the internal audit team:

a. Has the collective internally and externally sourced capacity, skill, capability and experience to execute the internal audit plan and influence stakeholders across the organisation.

b. Has a balance of team members commensurate to the size and complexity of the organisation, that possesses between them:

i. Accreditations by a professional body or professional certification as an internal auditor;

ii. Business experience in the organisation or peer organisations;

iii. Qualifications or experience in related disciplines, including, but not limited to, finance, data analytics, information technology and risk management. Some internal audit team members may also have qualifications or experience in project management, organisational psychology, investigations or leadership;

iv. Capabilities relevant for influencing stakeholders, including, but not limited to, the ability to deliver clear and concise verbal and written communication, as well as skills in negotiation, conflict resolution, governance and change management;

v. In addition, all team members should possess personal attributes of courage and resilience and apply and uphold the principles of integrity, objectivity, confidentiality and competency (as required by the IIA's Code of Ethics).

c. Implements or endorses a talent management program, to attract and retain key internal audit talent.

Commentary:

The composition of the internal audit team should take into account the assurance needs of an organisation's stakeholders and business objectives, strategies, associated risks and risk management processes, operations, programs, systems and controls. The mix of knowledge, skills and competencies should dynamically respond to changing business objectives, risks and stakeholder assurance needs.

To achieve this, the CAE should consider the use of internal audit team resources, internal capabilities (such as technical subject matter experts), seconded or procured resources from elsewhere in the organisation and external co-sourced capabilities.

The maintenance of skill, capability and experience in an internal audit team should be achieved through a mix of relevant training programs, supporting team members to undertake postgraduate or professional accreditations, ongoing recruitment, secondment from other parts of the organisation and co-sourcing with external third parties.[7]

A comprehensive talent management program is recommended to attract and retain key internal audit talent.

Where internal resources are used, there should be an individual development plan for each team member to build and maintain his or her skills and capabilities in line with the risks of the organisation and the internal audit team's strategic direction. Each team member should receive coaching and feedback on a periodic basis and meet the organisational compliance obligations.

Where an external co-source resource is used, the audit activities should be subject to the same quality assurance work as the internal resources.

IIA Standard (IPPF) references:

1210 – Proficiency

1230 – Continuing Professional Development

2030 – Resource Management

Recommendation 2.2

The adequacy of resourcing in the internal audit team to provide effective challenge to the organisation should be reviewed by the Audit Committee at least annually.

Commentary:

To inform the Audit Committee review, the CAE should provide the Audit Committee with a recommendation on the sufficiency of resourcing based on the skills required to conduct the work needed (refer to Recommendation 2.1, above) and whether the internal audit budget is sufficient to recruit and retain staff or procure other resources with the expertise, experience and objectivity necessary to provide effective challenge throughout the organisation and to the leadership team.

IIA Standard (IPPF) references:

2020 – Communication and Approval

2030 – Resource Management

2060 – Reporting to Senior Management and the Board

Recommendation 2.3[8]

The CAE should have a level of seniority within the organisation to allow appropriate access to information and the authority to challenge the leadership team.

Subsidiary, branch and individual heads of internal audit should be at a level of seniority comparable to the senior management whose activities they are responsible for auditing.

Commentary:

To facilitate appropriate challenge of the leadership team and senior management, internal audit team members should possess commensurate standing to the stakeholders involved in the activities which they are responsible for auditing. Internal audit should have the right to attend and observe all, or part of, the leadership team meetings and any other key management decision-making and governance fora.

IIA Standard (IPPF) references:

1000 – Purpose, Authority, and Responsibility

7 Comparable to paragraph 21 of the CIIA Guidance on Effective Internal Audit in the Financial Services Sector, 2nd edn, September 2017 (the UK Code)
8 Refer to Recommendation 1.2

Recommendation 2.4

Where the tenure of the CAE exceeds a predetermined timeframe, the Audit Committee should perform an annual assessment of the ongoing independence and objectivity of the CAE.

Commentary:

Based on the appetite of the organisation, where the tenure of the CAE exceeds a predetermined timeframe, the Audit Committee should perform an annual assessment of the ongoing independence and objectivity of the CAE.

The Committee notes that current tenure practices vary across the financial services industry. Most Australian entities do not have a CAE tenure policy, instead relying upon auditor independence policies. Of those entities which do have predetermined CAE tenure policies, some align with external audit engagement partner rotation requirements (five years), some use the International Federation of Accountants *Handbook of the Code of Ethics for Professional Accountants*, which also aligns with the UK Code (seven years), some refer to the ASX Corporate Governance Council's *Corporate Governance Principles and Recommendations* (ten years) and others have determined their own entity policies for CAE tenure (e.g. eight years).

Each entity should develop its own CAE tenure policy and, upon reaching that tenure, on an annual basis, consider whether requiring a change of CAE is in the best interests of the entity and its stakeholders, having regard to the likely future performance, independence and objectivity of the incumbent CAE relative to the alternative CAE options.

Recommendation 2.5

The internal audit charter and the Audit Committee charter should outline the performance assessment process for the CAE and should ensure the Audit Committee Chair approves the CAE's performance objectives, provides performance feedback, and approves the CAE's performance ratings.

Commentary:

The performance assessment process for the CAE and any subsidiary, branch and individual heads of internal audit should be outlined in the internal audit charter and the Audit Committee charter.

To elevate the independence and objectivity of the CAE, the Chair of the Audit Committee should approve the objectives of the CAE, provide performance feedback at least annually, and approve the CAE's performance rating. The objectives and performance appraisal process would also generally take into account the views of the Chief Executive Officer and other senior management and should be consistent with individual accountabilities.

Many CAEs of financial services organisations will be 'accountable persons' under either the Banking Executive Accountability Regime (BEAR) or the Financial Accountability Regime (FAR).

Irrespective of whether BEAR or FAR applies, the CAE, along with any subsidiary, branch and individual heads of internal audit, should have a clear statement of individual accountability, clearly stating his or her responsibilities. The statement should describe the actions, decisions and outcomes for which the individual is accountable and the part(s) of the organisation to which the accountabilities relate. This statement should be approved by the Audit Committee Chair and be revised promptly upon any change in the incumbent or any change in the accountabilities. Acceptance of individual accountability should be indicated in the form of a signed document with an effective date.

Material failure to meet expectations outlined in individual accountability statements and annual performance objectives should lead to direct and proportional consequences, which could include reduction in base salary or variable remuneration, loss of seniority, and dismissal in the most extreme case. The IIA-Australia Disciplinary & Review Committee also investigates complaints and determines disciplinary action for members who breach the IIA-Australia Constitution or By-laws or the IIA Code of Ethics.

Recommendation 2.6

The remuneration framework of the CAE and internal audit team should be structured in a manner which avoids conflicts of interest, does not impair independence and objectivity, and is not exclusively linked to the short-term performance of the organisation.

Commentary:

The remuneration framework of the CAE and internal audit team should be designed to comply with the current APRA Prudential Standard and Guidelines.

The Chair of the Audit Committee should be responsible for recommending the remuneration of the CAE to the Remuneration Committee.

Provide assurance which adds value

Internal audit should be effective and add value in meeting the assurance needs and expectations of the Board and stakeholders.

Recommendation 3.1

The CAE should provide the Audit Committee with an annual declaration which attests to the adequacy of internal audit activities and that the internal audit governance structure, annual plan, people model and reporting are appropriate to the organisation, having regard to the assurance needs of the Board and stakeholders, and the size, business mix and complexity of the organisation.

Commentary:

Most CAEs provide an annual attestation as to the fulfilment of the internal audit charter. Many financial services CAEs will also provide an annual attestation as to the fulfilment of their role accountabilities under the Banking Executive or Financial Accountability Regime.

To the extent that these attestations do not cover the following material, CAEs should provide a supplementary annual declaration or procure an independent review as to the adequacy and appropriateness of the internal audit activities. The annual declaration should confirm for the previous year ended, to the best of the CAE's knowledge and having made appropriate enquiries, in all material respects, that:

a. Internal audit has maintained its independence and conformed with the Institute of Internal Auditors' Code of Ethics, the Core Principles, the International Professional Practices Framework and the Internal Audit Better Practice Guide for Financial Services in Australia;

b. The internal audit plan, capability and resourcing are appropriate for the organisation, having regard to the assurance needs of the Board and stakeholders and the size, business mix and complexity of the organisation;

c. The key internal audit findings and observations have been accurately reported to management and the Audit Committee;

d. Management's proposed responses to key internal audit findings, set out as resolution actions either within or following the audit reports issued during the year, were adequate at the time of issuance; and

e. The key outcomes arising from any relevant internal audit observations of the status of agreed resolution actions for previously raised audit findings have been accurately reported to management and the Audit Committee.

In making the annual declaration, the CAE should have regard to the appropriate level of materiality for the organisation and stakeholders. Immaterial issues or non-compliances should not directly lead to a qualification of the declaration. However, the CAE may wish to include relevant matters of emphasis for the consideration of the Audit Committee. The disclosure of any such matters should be made with the purpose of assisting the Audit Committee to understand any organisation-specific limitations on the assurance provided by internal audit and thereby minimise any expectations gap.

In the event the CAE is unable to provide an unqualified annual declaration, a rationale should be provided to the Audit Committee which outlines the relevant qualifications or disclaimers and sets out a proposed action plan to close the identified gaps.

With regard to the declaration regarding the adequacy of management's proposed responses to key audit findings, the intention is only to highlight areas where there was material disagreement with management about the adequacy of agreed actions at the time of report issuance or where an agreed action has been unacceptably delayed. This part of the declaration is not intended to indicate whether or not management's actions have been implemented.

IIA Standard (IPPF) references:

2060 – Reporting to Senior Management and the Board

Recommendation 3.2

Internal audit should be effective and add value in meeting the assurance needs and expectations of the Board and other relevant stakeholders.

Commentary:

An understanding of the Board and other relevant stakeholders' expectations is fundamental to internal audit's ability to provide value. Internal audit adds value to the organisation and stakeholders when it provides objective and relevant assurance, and contributes to the effectiveness and efficiency of governance, risk management and control processes. Internal audit should add this value through the effectiveness of its relationships with the Board, management and other stakeholders, the quality and timeliness of its assurance reporting and recommendations and its independent contribution to the overall assessment of the risk and control maturity of the organisation.

Internal audit assurance reporting should be targeted to the areas which will add value to the Board and stakeholders involved in the development of the internal audit plan, particularly risk.[9]

IIA Standard (IPPF) references:

2000 – Managing the Internal Audit Activity

Recommendation 3.3

Internal audit's independence as an assurance provider and the objectivity of its work should be safeguarded.

Commentary:

Independence and objectivity form one of the IIA-Global's foundational Attribute Standards[10] and should be maintained at both an organisational and individual level.

While upholding its independence and objectivity, internal audit should utilise its capabilities to assist the organisation to improve risk culture, systems, processes and controls.

Accordingly, in some cases, it will be appropriate for internal audit to act as a trusted advisor, subject matter expert or investigator for the organisation. However, while internal audit may provide expert advice on the design of first and second line controls, the function must not take responsibility for their design, implementation or operation.

Internal auditors are statutory eligible recipients of whistleblower disclosures.[11] Accordingly, owning a whistleblower policy or process, or conducting an investigation of a matter raised by a whistleblower, is consistent with internal audit's role as an independent provider of assurance.

IIA Standard (IPPF) references:

1100 – Independence and Objectivity

Recommendation 3.4

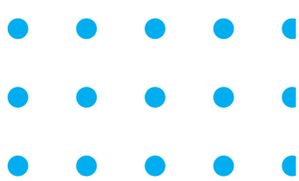
Internal audit should set a strategy which is approved by the Audit Committee.

Commentary:

Internal audit's vision and strategy should be approved by the Audit Committee and be communicated to the Board and other relevant stakeholders. The strategy should establish a methodology for conducting internal audits, including quality criteria and a provision for regular external benchmarking.

IIA Standard (IPPF) references:

2040 – Policies and Procedures



9 Refer also to Recommendation 1.5
10 Standard 1100 – Independence and Objectivity – IIA-Global Attribute Standards
11 Section 1317AAC of the Treasury Laws Amendment (Enhancing Whistleblower Protections) Act 2017

Recommendation 3.5

Internal audit's operational processes should be established and managed in accordance with the approved strategy.

Commentary:

The CAE should manage internal audit through:

- Periodic development of a comprehensive risk-based audit plan;
- Ensuring all internal audits are conducted in accordance with the established methodology and quality criteria;
- Regular engagement with key business stakeholders to understand business changes, seek input into the internal audit plan and advise on the progress of audits and material issues;
- Approval of the publication of any audit engagement reports, including recommendations for improvement;
- Setting key performance indicators in respect of internal audit;
- Reporting regularly to the Audit Committee and other relevant stakeholders on the outcomes of any audits, as well as the performance of internal audit itself;
- Ensuring the appropriate follow-up of material issues, including the effective resolution of their root causes;
- Implementing the organisation's risk and compliance framework in respect of the risk and compliance obligations of internal audit; and
- Escalating issues of concern to the Chief Executive Officer or Chair of the Audit Committee, where appropriate.

IIA Standard (IPPF) references:

2340 – Engagement Supervision

Recommendation 3.6

Establish and maintain capability to fulfil the audit strategy and annual internal audit plan.

Commentary:

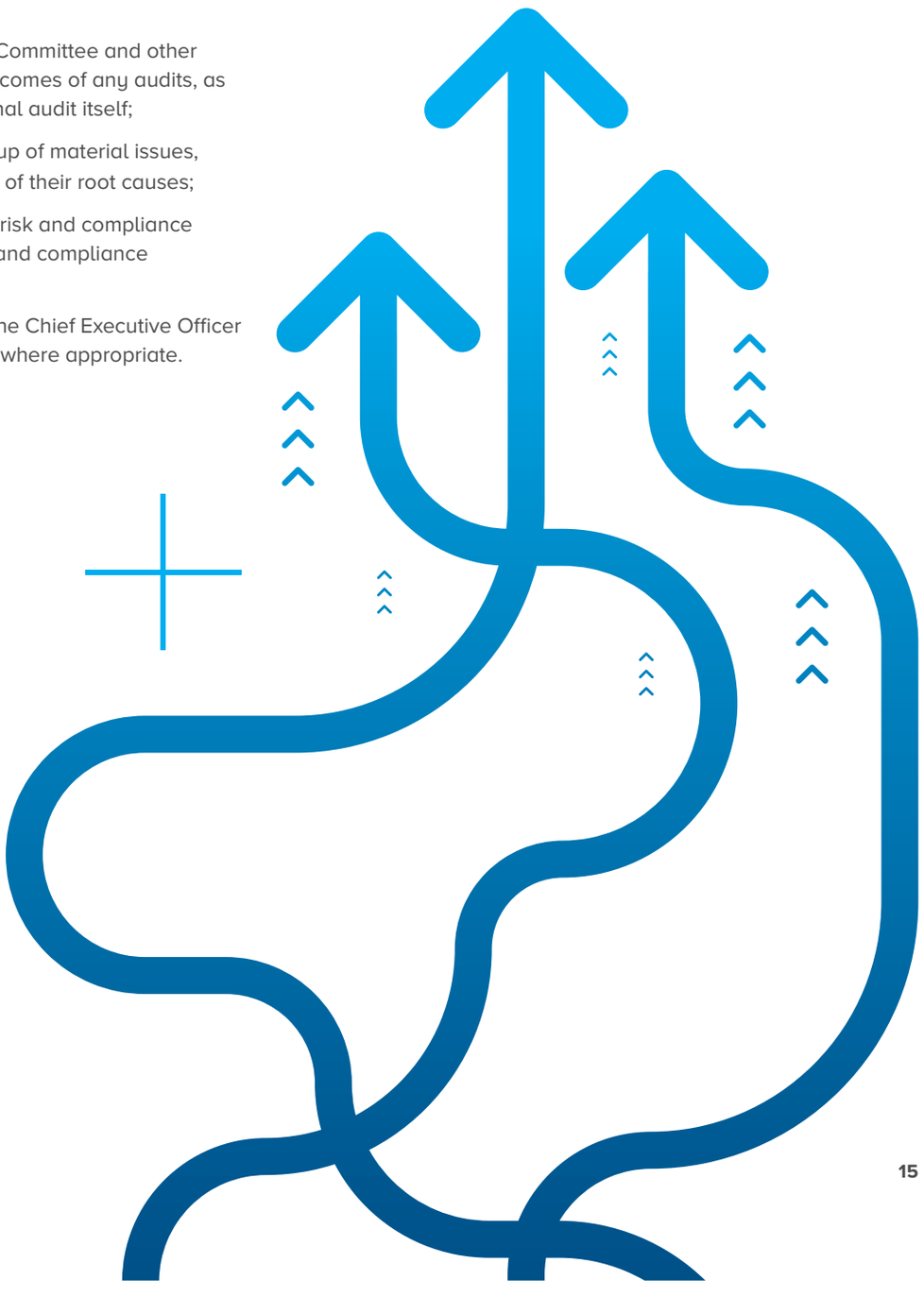
Establish an appropriately resourced internal audit team with the right mix of skills and competencies to deliver the audit strategy and annual plan. This may include the use of external co-sourced capabilities.[12]

IIA Standard (IPPF)references:

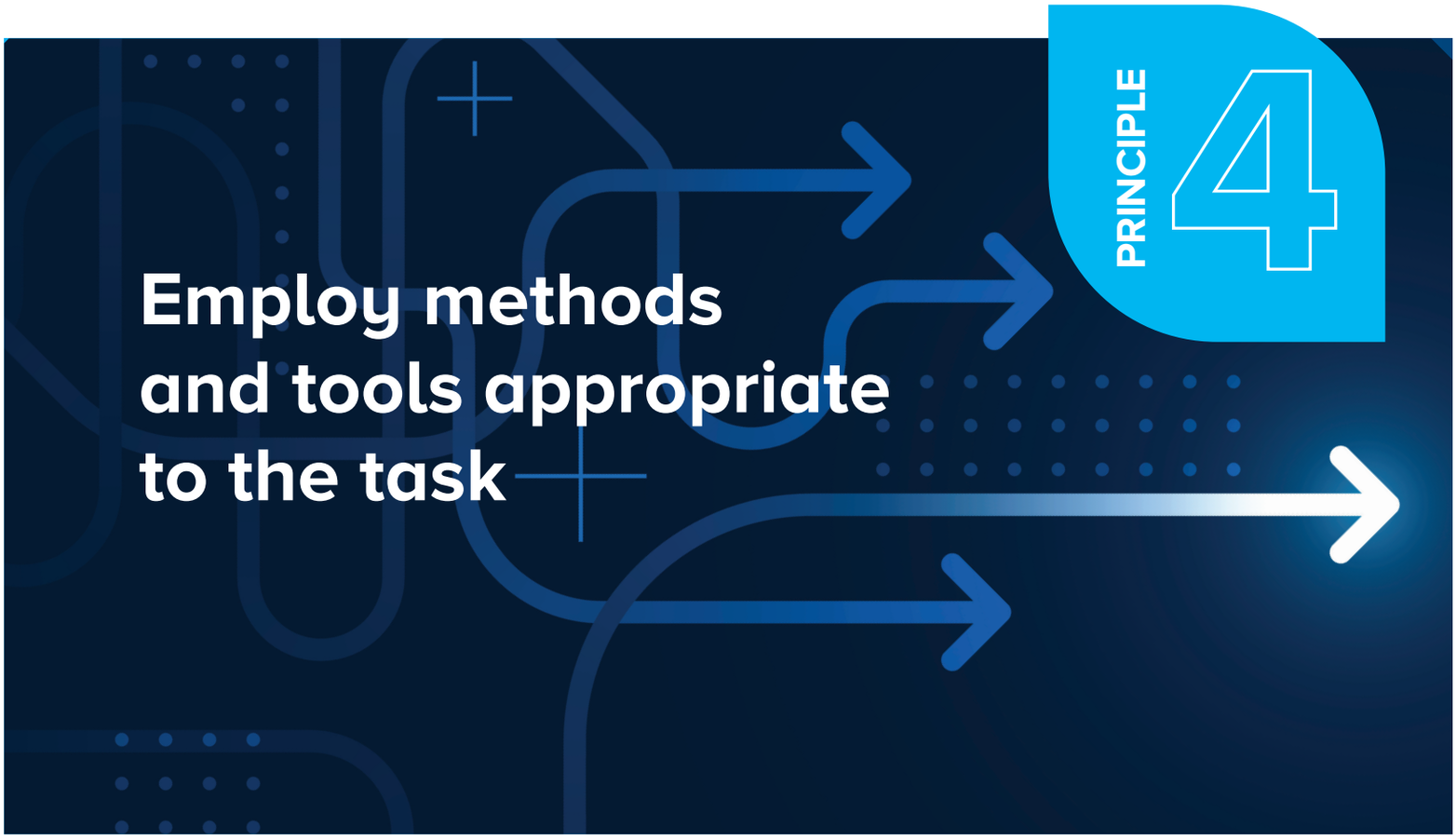
2030 – Resource Management

2050 – Coordination and Reliance

2230 – Engagement Resource Allocation



12 Refer to Recommendation 2.1



Internal audit should maintain an up-to-date methodology and underlying practices, and associated tools, to enhance its effectiveness.

Recommendation 4.1

Internal audit should maintain an up-to-date set of policies and procedures, and performance and effectiveness measures.

Commentary:

The policies and procedures should guide the internal audit activity, clearly articulate the audit methodology used, align with IIA Standards and guidance, reference the charter or mandate of the function, and refer to the audit techniques outlined in this guidance. In addition, it should cover the types of deliverables expected of internal audit, including the type of audit engagements, levels of assurance and associated opinions, issue significance ratings and management reporting.

Performance and effectiveness measures should be implemented and used to assess the effectiveness of internal audit.

IIA Standard (IPPF) references:

2040 – Policies and Procedures

Recommendation 4.2

Internal audit should have a structured, documented and risk-based continuous risk assessment (CRA) process, which is conducted and concluded upon periodically.

Commentary:

The CRA process should identify significant emerging and changing risks, including key internal factors (e.g. business changes, incidents and issues) and key external factors (e.g. industry and regulatory changes), confirm internal audit's assessment of risk across the business, and ensure the audit plan is focusing on material risks for the organisation.

The output of the CRA process should be documented and could include changes to risk assessments in the audit universe, changes to the audit plan, new audit issues raised, or key messages to the leadership team and/or Audit Committee. The audit plan should also have the flexibility (e.g. unallocated hours) to allow internal audit to prioritise work arising from CRA or from regulatory requests without negatively impacting the overall audit plan. Material changes to the audit plan should be approved by the Audit Committee.

The frequency of CRA will be driven by the size and nature of the organisation.

IIA Standard (IPPF) references:

2010 – Planning

2020 – Communication and Approval

Recommendation 4.3

Internal audit should:

a. **Consider applying data analytics (DA) throughout all phases of the audit cycle;**

b. **Assess data risk;**

c. **Begin by capturing and validating data in a timely fashion, prior to analysing the data; and**

d. **Implement training to ensure their internal audit staff have sufficient DA capabilities.**

Commentary:

Where appropriate and commensurate with the risk maturity of the organisation, internal audit should shift the focus from traditional sample-based audit procedures to an increasing focus on and utilisation of data analytics (DA), to increase the effectiveness and efficiency of its audit activities.

DA techniques usage will be dependent on the data quality and availability, the systems used to capture and process data, and the capabilities of internal audit. It will also be dependent on the extent of controls-based DA utilised by the first and second line management roles.

DA should be used throughout the audit life cycle and will become even more important as organisations increase their reliance on automation and the use of robotics and artificial intelligence.

During audit planning, internal audit should consider an assessment of data risk alongside other key risks and look to validate controls by evaluating the underlying data.

For DA to be successfully implemented, advanced planning is required so there is sufficient time to capture and validate the data before it is analysed. This includes identifying available data, extracting needed datasets, and testing the data quality using appropriate DA techniques.

DA can also be used for continuous monitoring or testing.

Ongoing skills assessments and training should be conducted to ensure the DA skills of internal audit are keeping pace with industry developments.

IIA Standard (IPPF) references:

1220 – Due Professional Care

Recommendation 4.4

Internal audit should have a robust root cause analysis methodology.

Commentary:

The root cause analysis methodology should consider both hard controls (e.g. policies and procedures, roles and responsibilities) and behavioural elements (e.g. clarity, commitment, achievability, and whether they are incentivised), and (at a minimum) should be applied to all significant audit-raised issues. This will ensure management action plans address the root cause of the issues raised, and hence result in more sustainable remediation outcomes for the organisation.

The root cause analysis should also assess whether the issue (and root cause) could be relevant to other areas of the organisation.

Recommendation 4.5

Internal audit should have a retrospective review/ 'lessons learned' process in place when the organisation is subject to significant incidents and regulatory actions.

Commentary:

The primary aim of retrospective reviews is to improve internal audit. The retrospective review should assess the adequacy of internal audit with reference to significant incidents and regulatory actions (including methodology and audit coverage). Internal audit should also assess whether the function could have identified significant external events impacting other institutions.

In addition, internal audit should verify whether the organisation has performed a 'lessons learned' exercise (i.e. assessed the first and second line management roles and considered whether any improvements in the control environment are required).

Recommendation 4.6

Internal audit should have a quality assurance program in place to ensure that the function operates in line with its policies and procedures.

Commentary:

Internal audit should develop a quality assurance capability, with the work performed by individuals who are independent of the delivery of the audit. The individuals performing the assessments should have the standing and experience to meaningfully challenge internal audit performance and to ensure that internal audit judgements and opinions are adequately evidenced.

The scope of the quality assurance review should include internal audit's understanding and identification of risk and control issues, in addition to the adherence to audit methodology and procedures. This may require the use of resources from external parties. The quality assurance work should be risk-based, to cover the higher risks of the organisation and of the audit process. The results of these assessments should be presented directly to the Audit Committee at least annually. Where internal audit is outsourced to an external provider, internal audit's work should be subject to the same quality assurance work as the in-house functions. The results of this quality assurance work should be presented to the Audit Committee at least annually for review.

IIA Standard (IPPF) references:

1300 – Quality Assurance and Improvement Program

1310 – Requirements of the Quality Assurance and Improvement Program

1311 – Internal Assessments

1320 – Reporting on the Quality Assurance and Improvement Program

Recommendation 4.7

Internal audit should place reliance (i.e. 'claim' audit coverage) on another assurance provider's work only after an evaluation of the effectiveness of the provider's work has been undertaken.

Commentary:

The reliance on other assurance parties to 'claim' audit coverage can result in more efficient audit engagements, allowing the function to allocate its resources to other areas of audit coverage. (Note: This recommendation is not applicable for work undertaken as part of a co-sourcing relationship where the internal audit function retains 'ownership' of the audit work (including scope and quality/review of workpapers).)

The effectiveness assessment should be performed at least every two years, and include an assessment of the following areas:

- Governance: mandate/charter, independence and objectivity;
- Purpose: independence and objectivity;
- Resourcing: capability and capacity to deliver on mandate;
- Competency;
- Policies and procedures (including quality assurance);
- Elements of practice;
- Reporting and issue remediation: Committee reporting; assurance reports; issue tracking and validation;
- Communication of results and impactful remediation.

A reliability opinion should be issued to conclude on this assessment, with issues raised as appropriate.

If the assurance provider is assessed as effective, and the scope of the assurance provider's work is aligned with some or all of the audit scope, then reliance can be placed on the assurance provider's work if reassurance work is performed to confirm internal audit would come to the same conclusion. This reassurance should involve risk-based sample re-performance of the work (process walkthrough, control design and operating effectiveness testing).

If issues are identified with the assurance work, internal audit should not place any reliance on the assurance provider's work and should proceed with direct testing of the audit scope, and raise any issue(s) regarding the assurance provider as appropriate.

Reassurance work should be documented in the audit file as per standard practice.

IIA Standard (IPPF) references:

2050 – Coordination and Reliance

Recommendation 4.8

Internal audit should be assessed on conformance with the Code of Ethics and the Standards by a qualified independent assessor from outside the organisation at least once every five years.

Commentary:

The Audit Committee should obtain an independent and objective external assessment at appropriate intervals, depending on the size and nature of the organisation. This could take the form of periodic reviews of elements of the function against best practice (of both domestic and global peers), or a single review of the overall function. In any event internal audit should as a minimum be subject to a review at least every five years, as set out in the International Professional Practice Framework for internal audit. The conformity of internal audit with this guidance should be explicitly included in this evaluation. The Chair of the Audit Committee should oversee and approve the appointment process for the independent assessor.

IIA Standard (IPPF) references:

1312 – External Assessments

PRINCIPLE 5

Report to influence positive change

Internal audit should drive positive change by providing timely, accurate and insightful information to be used as a basis for making risk-focused decisions.

Recommendation 5.1

Internal audit should provide formal reporting to the Audit Committee as well as other Board Committees as appropriate (e.g. Risk Committee, Technology Committee, Remuneration Committee, etc.). In addition, internal audit should provide formal reporting to the leadership team as appropriate.

Commentary:

Internal audit reporting should be formally documented and endorsed by the relevant governing bodies.

IIA Standard (IPPF) references:

2060 – Reporting to Senior Management and the Board
2440 – Disseminating Results

Recommendation 5.2

Internal audit should consider the following types of reporting:

- **Board and Board Committee (e.g. Audit Committee, Risk Committee, etc);**
- **Leadership team;**
- **Real time escalation (as required for critical issues);**
- **Standard internal audit reports;**
- **Targeted reviews;**
- **Thematic reviews;**
- **Project reviews;**
- **Limited reviews;**
- **Special reviews and investigations;**
- **Unrated reports; and**
- **Validation/follow-up reviews on management actions.**

Commentary:

The nature and content of the reporting will depend on the remits and needs of the respective governing bodies. In addition, consideration needs to be given to the appropriate timeliness of the reporting (i.e. raising significant issues immediately through a defined escalation protocol rather than waiting until a report is formally completed).

IIA Standard (IPPF) references:

2060 – Reporting to Senior Management and the Board
2440 – Disseminating Results

Recommendation 5.3

Regardless of the forum and format, formal internal audit reporting should have a standard structure.

Commentary:

Commensurate with the risk maturity of the organisation, internal audit reports should consider including the following:

- An overall rating supporting the holistic assessment;
- A first page that includes all the key information a CEO or division head needs to know, e.g. holistic rating, issue statistics by rating, an insightful executive summary including significant themes and issues which justify the holistic assessment;
- Issue ratings which align to required Board and management attention, ownership and accountability. These ratings should be applied consistently;
- Detailed 'significant'/key issues (specifically highlighting when issues are repeated or reopened). Where significant/key issues or themes have been identified, the reporting should be compelling, such that management take timely action to effect positive change;
- A summary of known effectively managed issues;
- Details of other reportable issues;
- Scope;
- Background;
- A distribution list highlighting the Banking Executive Accountability Regime (BEAR) primary accountable person(s);
- Issues raised clearly and concisely, covering:
  - Issue rating
  - Issue details (specifically highlighting if issues are repeated or reopened)
  - Root cause
  - An impact statement aligned to rating
  - Recommendation and/or agreed actions with appropriate due dates, confirming that these will address the underlying risk sustainably.
  - An embedded or accompanying management response should generally be included.

Where an issue may suggest a regulatory breach has occurred, internal audit must liaise with the relevant part of the organisation (e.g. often compliance) for their consideration as to whether to add the incident to the 'breach register'. Maintaining a breach register is considered best practice by Australian financial services regulators.

- Specialised reporting that is sufficient to allow appropriate judgement;
- A focus on key risks and key control failures – audit departments often lose impact and at times their reputation by raising issues of such low risk that they distract management from true risks and concerns.

IIA Standard (IPPF) references:

2410 – Criteria for Communicating

2450 – Overall Opinions

Recommendation 5.4

To contribute to effective organisational governance, appropriate Board Audit Committee reporting and protocols are required.

- Reporting to the Board Audit Committee and approvals required from the Audit Committee Chair should, at a minimum, include the following:
  - Audit department charter review and approval
  - Annual audit plan for approval
  - Budget approval
  - Results of key audits and issues
  - Periodic reporting of overdue and longstanding issues exceeding preestablished time thresholds based on ratings. The relevant executive should attend and discuss these, based on Board preferences
  - Effectiveness of internal audit, e.g. QA results, KPIs, stakeholder surveys, incident post-mortems, etc.
- Where issue remediation dates can be changed, the Audit Committee Chair should be consulted to determine if they wish to approve all changes to significant issue remediation dates applicable to their jurisdiction. Similarly, the Audit Committee Chair should be consulted to determine if they wish to review remediation date changes to significant issues outside, but relevant to, their jurisdiction so they have the opportunity to highlight any concerns to the relevant group Audit Committee.
- The Audit Committee Chair should be consulted to determine if they wish the relevant executive to attend and discuss (red/unsatisfactory) internal audit reports for which they are responsible.

Recommendation 5.5

Where appropriate, internal audits performed may result in input to the organisational performance management process, including consequence management, with the objective of reinforcing and rewarding appropriate conduct and addressing inappropriate conduct.

Commentary:

The identification and prompt remediation of issues must be encouraged. As such, the proportionate use of the organisational performance management framework is essential, based on the individual circumstances identified.

Confirmation of performance management consideration

Internal audit must confirm that a fair and effective process exists for all staff referred by internal audit for performance management consideration – both positive and negative. The chief internal auditor should be advised of the impact/ outcomes of all internal audit performance management consideration referrals made.

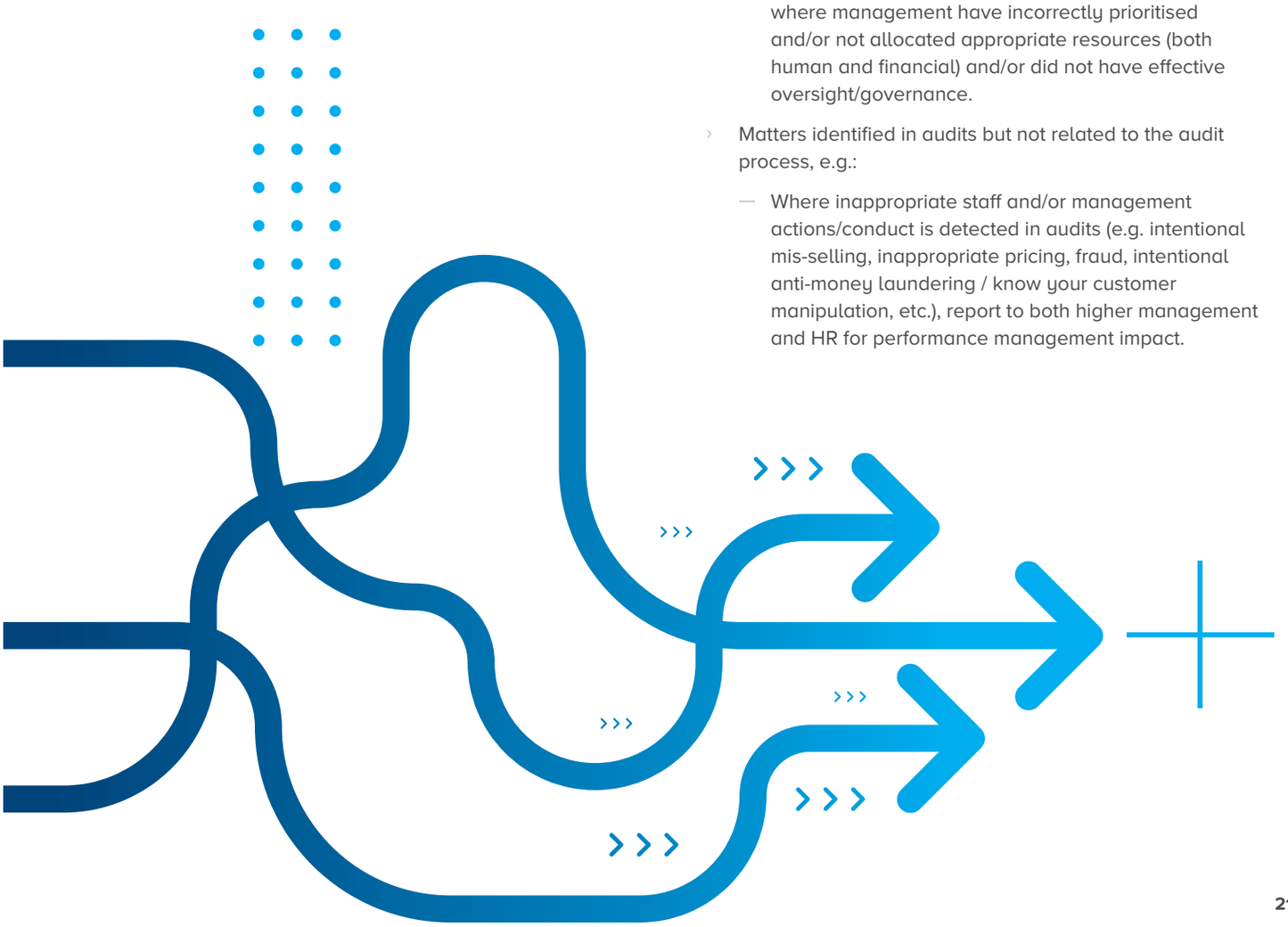
Examples of positive performance management

- Strong proactive risk identification and appropriate key controls;
- Management self-identified issues surrounding key risks; and
- Exemplary conduct with a focus on continuous improvement and proactive issue remediation.

Examples of negative performance management

Negative performance management may arise in two distinct ways, as follows:

- Audit-related examples, including:
  - Where an unsatisfactory, or equivalent, rated report is issued, and management were not aware of the significant issue(s) raised which drove the rating. The underlying cause will be the determinant as to whether negative performance management should occur.
  - Obstructive or inappropriate staff conduct during audit execution;
  - Lack of sustainability, i.e. repeated or reopened material issues surrounding key risks, where no extenuating circumstances exist; and
  - Overdue issues (beyond a reasonable time threshold) without justifiable extenuating circumstances e.g. where management have incorrectly prioritised and/or not allocated appropriate resources (both human and financial) and/or did not have effective oversight/governance.
- Matters identified in audits but not related to the audit process, e.g.:
  - Where inappropriate staff and/or management actions/conduct is detected in audits (e.g. intentional mis-selling, inappropriate pricing, fraud, intentional anti-money laundering / know your customer manipulation, etc.), report to both higher management and HR for performance management impact.



Adopt appropriate methodologies for auditing risk culture

The responsibility for setting risk culture sits with the organisation's Board. Organisational management then has the accountability for driving that risk culture through the organisation, measuring and reporting on risk culture and determining actions to address any gaps. As an independent function, internal audit can provide independent assurance on the governance processes around risk culture and reporting, but also an independent view of the risk culture itself. Internal audit provides assurance in relation to risk culture both through 'business as usual' audits and broader risk culture audits.

Recommendation 6.1

Since risk culture is a fundamental component of the risk management framework, in its 'business as usual' audits, whether of a business unit, a process or a review of a risk event, IA should consider the (risk) cultural dimension.

a. **Given its independent role in the organisation, IA provides a crucial perspective on the organisation's risk culture;**

b. **Where the first or second line are performing risk culture assessments, internal audit should challenge these assessments as necessary;**

c. **Internal audit should use a variety of techniques to produce risk culture insights in its audit activities;**

d. **These risk culture insights should be presented in audit reports where relevant, including, for APRA-regulated entities, the annual review of the risk management framework; and**

e. **Risk culture insights should be reported to management and the Audit Committee on a regular basis.**

Commentary:

Risk culture, an aspect of the overall organisational culture, refers to the norms of behaviour in an organisation relating to risk management. Risk culture is a crucial element within the risk management framework. The Board must ensure that it forms a view of the risk culture in the institution, and the extent to which that culture supports the ability of the institution to operate consistently within its risk appetite, identify any desirable changes to the risk culture and ensure that the institution takes steps to address those changes. (CPS220, paragraph 9(b)). (Superannuation entities should refer to SPS220, paragraph 22(f)).

A favourable risk culture means that employees go beyond 'mere' compliance with risk policies to being committed to them: there is open and regular discussion of risk; concerns about business practices are raised and acted upon promptly; and risk management is seen as an enabler of organisational success. An unfavourable risk culture can compromise the effectiveness of the risk management framework because compliance with policy is not seen as a genuine priority for the organisation; other activities, such as generation of short-term profits, can override risk management considerations.

Since risk culture is a fundamental component of the risk management framework, internal audit departments should aspire to consider risk culture in audits, whether of a business unit, a process or a review of a risk event. That is, internal audit will, as a matter of course, consider the underlying behavioural factors that may be producing observed outcomes. Alternatively, where this is not possible due to resource constraints, a risk-based approach could be used to determine which audits will include consideration of risk culture.

6.1.a Given its independent role in the organisation, internal audit provides a crucial perspective on the organisation's risk culture.

The Board has the responsibility to form a view of the risk culture in a financial institution (CPS220, paragraph 9(b) and CPG220, paragraph 21). Risk culture, referring to perceived behavioural norms, is inherently difficult to assess and may vary across an organisation. Directors, especially non-executive directors (NEDs), may have difficulty forming an accurate picture of the behavioural norms of the organisation.

Internal audit is ideally placed to observe everyday business practices and informal communications that shed light on the actual, as opposed to the desired, risk culture. Internal audit is also ideally placed to investigate risk issues and policy breaches, uncovering the underlying behavioural drivers that may point to risk culture issues. Accordingly, internal audit is a vital source of intelligence for the Board with regard to risk culture.

6.1.b Internal audit should challenge the risk culture assessments of first and second line management roles as necessary.

In some financial institutions, first and second line management conduct their own assessments of risk culture. Due to the difficulty of assessing risk culture noted above, it is important that internal audit provide its own perspective. Internal audit should report on any inconsistencies identified between the various assessments, challenging both the methodology and the conclusions, as necessary.

6.1.c Internal audit should use a variety of techniques to audit risk culture.

Internal audit should use a variety of techniques to evaluate risk culture. To achieve this goal, it may be necessary to widen the expertise of the internal audit team, as noted in Principle 2. Useful risk culture insights may be gleaned from a range of techniques, including:

- Interviews and focus groups;
- Observation of behaviours, including at meetings;
- Anonymous staff surveys to quantify the perceptions of risk culture in practice;
- Analysis of data related to customer outcomes (e.g. number/nature of complaints, time taken to resolve complaints, customer turnover, etc.);
- Analysis of data related to performance reviews, reward and consequence management (e.g. variation in manager ratings, suitability of consequences where misconduct is identified, etc.);
- Analysis of data relating to risk management effectiveness (e.g. risk appetite breaches, control failures, events and regulatory breaches, and timeliness of issue remediation)
- Analysis of data from staff (e.g. exit interviews, employee rating sites, staff turnover, use of confidential hotlines, etc.);
- Analysis of risk/issue reporting and the reasons for underreporting and repeat/recurring issues;
- Root cause analysis of major risk events;
- Data analytics (e.g. of emails, social media, textual analysis of complaints, etc.);
- Comparison of key documents (e.g. business plans, meeting agendas, mission statements, policy documents) to check for the degree of interconnectivity and consistency with which they address risk culture; and
- Evaluation of how people behave during an audit (whether they take accountability, are transparent, deny, deflect or discredit, etc.).

With regard to methodology, internal audit should be wary of survey methodologies that do not have a scientific basis. Problematic practices that may produce invalid results include:

- Use of survey items that have not been through a rigorous validation process, particularly where they have been developed in-house;
- Use of surveys that are too short to reliably capture all the necessary dimensions of risk culture;
- Including risk culture questions in the employee engagement survey, especially when engagement is a management KPI;
- Surveys that are invitational (everyone gets a unique link), so employees don't feel safe to give honest responses; and
- Reporting of results for small teams, so once again employees don't feel safe to give honest responses.

6.1.d Risk culture insights should be presented in internal audit reports as relevant, including, for APRA-regulated entities, the annual review of the risk management framework.

6.1.e Risk culture insights should be reported to management and the Audit Committee on a regular basis.

Every audit report, whether of a business, a process or a review of a risk event, is an opportunity for internal audit to provide vital risk culture insights. A discussion of risk culture should be included in reports wherever relevant. This is because risk culture is likely to vary across the organisation, and risk events typically have an underlying (risk) cultural element.

Consistent with CPS220, paragraph 44, an APRA-regulated financial institution should conduct an annual review of the effectiveness of its risk management framework. Given the importance of risk culture, internal audit should include, in this annual review, an overview of its findings on risk culture.

Regardless of regulatory status, internal audit should be reporting risk culture insights to management and the Audit Committee on a regular basis.

Recommendation 6.2

Internal audit should conduct audits of the risk culture framework on a cyclical basis consistent with the risk appetite of the organisation, or sooner if circumstances change substantially or if a self-assessment is requested by the regulator. An audit of the risk culture framework would involve assessing:

a. **The framework and process for setting the desired risk culture from the Board, and the way that has been communicated throughout the organisation;**
b. **The policies and procedures in place (in particular those dealing with risk, people and conduct) to ensure that they align with and support a favourable risk culture;**
c. **The process by which the organisation monitors and reports on its actual risk culture and what actions are taken when the actual risk culture is not consistent with the desired risk culture; and**
d. **The actual risk culture of the organisation, either as a whole or in part, including observations from past 'business as usual' audits.**

Commentary:

An audit of risk culture should be conducted periodically as determined by risk appetite and/or regulatory requirements. An unscheduled audit of risk culture would be indicated if a self-assessment is requested by the regulator or if there is a significant change in circumstances such as a change in leadership/strategy. Such a targeted audit of risk culture may also be prompted by serious and unexpected adverse business outcomes, or if the Chair of the Audit Committee, the Chair of the Risk Committee, or the CAE judges for any reason that such an audit is needed. An audit of the risk culture framework would involve reviewing:

- The process for setting the desired risk culture from the Board, and the way that it has been communicated throughout the organisation (e.g. has there been proper dissemination or just an email? Is there an effort to get staff to understand what it means for them, or is it just assumed that everyone knows what is expected of them?). Is the desired risk culture consistent with business strategy? Do formal statements of risk culture/values adequately capture the dimensions of risk (i.e. long-term resilience) and customer outcomes?
- The policies and procedures in place in an organisation, to ensure that they align with and support the desired risk culture set by the Board (e.g. code of conduct, staff training programs, capital adequacy, risk-adjusted performance measurement, risk reporting and analytics, compliance, and regulatory reporting systems, remuneration, business decisions, delegations of authority, recruitment, performance management, etc.). Is appropriate priority given to non-financial risks (operational, compliance, conduct)? Are risk/compliance functions adequately resourced? Are management action plans put in place to achieve the desired risk culture, including monitoring and assessing their effectiveness.
- The process by which the business (first and second line management roles) measures, monitors and reports on risk culture (as above, ensuring that there is a robust methodology in place, etc.), as well as how it is reported to the Board, and what actions are taken when the results show the culture isn't where it should be.
- The actual risk culture in the organisation or business unit: see discussion in 6.1.c with regard to various techniques to audit risk culture.

Appendices

Appendix A
Internal audit operating models

There are several operating models which are utilised across organisations in Australia to implement internal audit. The recommendations in this Better Practice Guide have been developed to apply broadly across all internal audit operating models.

In-House Internal Audit	The in-house model is provided exclusively or predominantly by in-house staff and managed in-house by an employee of the organisation. The Chief Audit Executive (CAE) or equivalent will have accountability to the Audit Committee for the delivery of internal audit activities.
Co-sourced Internal Audit	The co-sourced internal audit model is often conducted by a combination of in-house staff and service providers and managed in-house by an employee of the organisation, generally the CAE. It is acknowledged that the co-sourced model operates on a continuum and may vary between organisations. This can range from an engagement of subject matter experts to deliver or inform specific internal audits, the sharing or collaboration of resources on internal audits with service providers, or the entire outsourcing of individual internal audits within the internal audit plan.
Outsourced Internal Audit	The outsourced internal audit model sees internal audit services provided by a sole service provider or a panel of service providers contracted to the organisation, with no in-house function present. The service provider is actively managed by an employee with knowledge and experience of internal auditing, often referred to as the internal audit sponsor, while the outsourced provider is directly accountable to the Audit Committee for internal audit activities.

Appendix B
The Three Lines Model

The Three Lines Model, as outlined by the IIA's Three Lines Model Paper (dated 20 July 2020), is a guide to help organisations identify structures and processes that best assist in the achievement of objectives and facilitate strong governance and risk management. The principle-based model recognises that organisations differ considerably in their distribution of responsibilities and does not intend to mandate a structure, but rather to provide guidance on roles and responsibilities within the model to support effective risk management and governance. Internal audit is a third line role, which ensures independent and objective assurance and advice on all matters related to the achievement of objectives.

First Line Roles *(Management)*	› Lead and direct actions (including managing risk) and application of resources to achieve the objectives of the organisation. › Maintain a continuous dialogue with the governing body and report on planned, actual, and expected outcomes linked to the objectives of the organisation; and risk. › Establish and maintain appropriate structures and processes for the management of operations and risk (including internal control). › Ensure compliance with legal, regulatory and ethical expectations.
Second Line Roles *(Risk management and Compliance)*	› Provide complementary expertise, support, monitoring and challenge related to the management of risk, including: › The development, implementation and continuous improvement of risk management practices (including internal controls) at a process, systems and entity level. › The achievement of risk management objectives such as compliance with laws, regulations and acceptable ethical behaviour; internal control; information and technology security; sustainability; and quality assurance. › The provision of analysis and reports on the adequacy and effectiveness of risk management (including internal control).
Third Line Roles *(Internal audit and objective assurance)*	› Maintain primary accountability to the governing body and independence from the responsibilities of management. › Communicate independent and objective assurance and advice to management and the governing body on the adequacy and effectiveness of governance and risk management (including internal control) to support the achievement of organisational objectives and to promote and facilitate continuous improvement. › Report impairments to independence and objectivity to the governing body and implement safeguards as required.

Appendix C
Glossary of terms

Add value	Internal audit adds value to the organisation and stakeholders when it provides objective and relevant assurance, and contributes to the effectiveness and efficiency of governance, risk management and control processes.
Assurance service	An objective examination of evidence for the purpose of providing an independent assessment on governance, risk management and control processes for the organisation.
Audit Committee	A subcommittee to which the Board has delegated certain functions. The Audit Committee is responsible for the oversight of internal audit's conformance with the Code of Ethics, the IIA Standards and audit standard.
Audit engagement	A specific internal audit assignment, task or review activity such as an internal audit, control self-assessment review, fraud examination or consultancy.
Audit universe	A list of all auditable entities in an organisation. An auditable entity could be a location, department, function, financial statement area, compliance requirement, or a multitude of other entities.
Chief Audit Executive	Also known as the Head of Internal Audit, Chief Audit Executive (CAE) describes the role of a person in a senior position responsible for effectively managing internal audit in accordance with the internal audit charter and mandatory elements of the IPPF. Any reference to the CAE should be taken to include the 'CAE equivalent' in an outsourced internal audit function.
Code of Ethics	The Code of Ethics of IIA sets out principles relevant to the profession and practice of internal auditing, and rules of conduct that describe behaviour expected of internal auditors.
Compliance	Adherence to policies, plans, procedures, laws, regulations, contracts, or other requirements.
Conflict of interest	Any relationship that is, or appears to be, not in the best interest of the organisation. A conflict of interest would prejudice an individual's ability to perform his or her duties and responsibilities objectively.
Control environment	The attitude and actions of the leadership team regarding the importance of control within the organisation. This provides the discipline and structure for the achievement of the primary objectives of the system of internal control.
Core Principles	The Core Principles for the Professional Practice of Internal Auditing are the foundations for the IPPF and support internal audit effectiveness.
External co-sourcing	Engaging/employing a person from a firm outside the organisation who has special knowledge, skill and experience in a particular discipline.
Governance	The combination of processes and structures implemented by the Board to inform, direct, manage and monitor the activities of the organisation toward the achievement of its objectives.

Independence	The freedom from conditions that threaten the ability of internal audit to carry out internal audit responsibilities in an unbiased manner.
Internal audit charter	A formal document that defines internal audit's purposes, authority and responsibility. It establishes internal audit's position within the organisation; authorises access to records, personnel and physical properties relevant to the performance of engagements; and defines the scope of internal audit activities.
Internal audit	A department, division, team of consultants or other practitioners that provides independent, objective assurance and consulting services designed to add value and improve the organisation's operations. Internal audit helps an organisation accomplish its objectives by bringing a systematic, disciplined approach to evaluating and improving the effectiveness of governance, risk management and control processes.
International Professional Practices Framework	The conceptual framework that organises the authoritative guidance promulgated by the IIA. Authoritative guidance is composed of two categories: (1) mandatory, and (2) recommended.
Leadership team	Also known as the C-suite, senior management or executive management, the leadership team refers to the senior management team within the organisation and is overseen by the Board of Directors.
Objectivity	An unbiased mental attitude that allows internal auditors to perform engagements in such a manner that they believe in their work product and no quality compromises are made.
Policies and procedures	The policies and procedures guide internal audit. The form and content of the policies and procedures will be dependent on the size and nature of internal audit.
Risk	The possibility of an event occurring that will have an impact on the achievement of objectives. Risk is measured in terms of impact and likelihood.
Risk appetite	The level of risk that an organisation is willing to accept.
Risk culture	Risk culture, an aspect of the overall culture, refers to the norms of behaviour within an organisation relating to risk management. These norms, linked to underlying values and assumptions, determine the collective ability to identify, understand, openly discuss and act on the organisation's current and future risk.
Risk management	A process to identify, assess, manage and control potential events or situations to provide reasonable assurance regarding the achievement of the organisation's objectives.
Standard	A professional pronouncement promulgated by the International Internal Audit Standards Board that delineates the requirements for performing a broad range of internal audit activities and for evaluating internal audit performance.
Tone from the top	In the context of risk governance, tone at the top refers to the risk culture that exists in the Board and among senior executives. Tone at the top can be significant for determining risk culture throughout the organisation. Formal statements of values and policies may indicate tone at the top, but it is also reflected in the behaviour of directors and executives in relation to risk management, e.g. taking ownership of risk appetite, challenging business practices, allocating rewards and consequences, supporting second and third line functions.

IIA Financial Services Committee

The Committee was convened in August 2019. It brings together various businesses, internal audit practitioners, Audit Committee members and regulators, each offering valuable insights and expertise on internal audit issues and practices. Its primary work has been the development of this Better Practice Guide.

Committee members

Sandra Birkensleigh (Chair)
Non-Executive Director and Chair of the Financial Services Committee

Sue Carter
Non-Executive Director, First State Super

Deborah Chesney
Chief Audit Executive, Allianz Australia

Nicola Rimmer-Hollyman
Chief Audit Executive, AMP

Scott Kieran
General Manager, Chief Audit Executive, Group Audit, Westpac Group

Richard Knox
Head of Professional Practices, Macquarie Group

John F Minz
Non-executive Director and Chair of Audit Committees, RACQ Group

Amanda Morgan
Chief Audit Officer, Rabobank Australia & New Zealand

Professor Elizabeth Sheedy
Macquarie Business School

Jon Tyers
General Manager Audit, MLC Life Insurance

Muir Watson
Executive General Manager, Internal Audit, IAG

Observers

Brian Burgess
Operational Risk Specialist, Operational Resilience, APRA

Kim Demarte
Lead Supervisor, Governance, ASIC

Peter Jones
Chief Executive Officer, IIA-Australia

Doug Niven
Chief Accountant, ASIC

Elizabeth Parsons
Head of Operational Risk, Operational Resilience, APRA

Tony Rasman
Public Affairs Manager, IIA-Australia

Rob Sharma
Head of Accounting, Advice & Approvals, APRA

Acknowledgements

IIA-Australia acknowledges the contributions to this publication generously provided by:

Hanny Hassan
Partner, EY

Cindy Martin
Associate Director, KPMG

Damien O'Meara
Partner, EY

Pushpinder Singh
Partner, KPMG

Alex Timpers
Director, EY

IIA-Australia also acknowledges the use of material contained in the Chartered Institute of Internal Auditors (UK) Effective Internal Audit in the Financial Services Sector – Recommendations from the Committee on Internal Audit Guidance for Financial Services (July 2013 and 2017).

Further information about the Committee is available from IIA-Australia.

About the Institute of Internal Auditors

The Institute of Internal Auditors (The IIA) is the global professional association for internal auditors, with global headquarters in the USA and affiliated Institutes and Chapters throughout the world, including Australia (IIA-Australia).

As the chief advocate of the internal audit profession, The IIA serves as the profession's international standard-setter, sole provider of globally accepted internal auditing certifications, and principal researcher and educator.

The IIA sets the bar for internal audit integrity and professionalism around the world with its International Professional Practices Framework (IPPF), a collection of guidance that includes the International Standards for the Professional Practice of Internal Auditing and the Code of Ethics.

Copyright

Disclaimer

November 2020

The Institute of
Internal Auditors
Australia

T 02 9267 9155
E enquiry@iia.org.au

www.iia.org.au